(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2002 年4 月4 日 (04.04.2002)

PCT

(10) 国際公開番号
WO 02/27501 A1

(51) 国際特許分類[7]: G06F 12/14, 12/00, 13/00

(21) 国際出願番号: PCT/JP00/06420

(22) 国際出願日: 2000 年9 月20 日 (20.09.2000)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 および
(72) 発明者: 保倉 豊 (YASUKURA, Yutaka) [JP/JP]; 〒151-0072 東京都渋谷区幡ヶ谷一丁目11番13号-506 Tokyo (JP).

(74) 代理人: 関 正治(SEKI, Masaharu); 〒102-0076 東京都千代田区五番町4番地 幸ビル4階 Tokyo (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

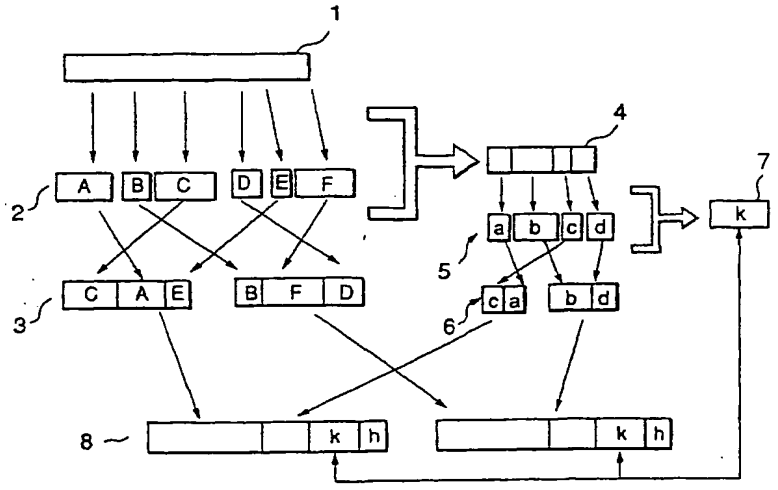
(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: METHOD OF EDITING/RESTORING ELECTRONIC INFORMATION

(54) 発明の名称: 電子情報の編成復元方法



(57) Abstract: An electronic information file (1) is divided into a plurality of information elements (2), which are combined in different orders to generate two or more information blocks (3) and to generate a primary distribution information file (4) holding information on the method for dividing/rearranging the information elements (2). Like the electronic information file (1), the primary distribution information file (4) is divided into key fragments (5) and rearranged to generate key blocks (6) and to generate a secondary distribution information file (7) holding information on the method for dividing/rearranging the primary distribution information file (4). The information blocks (3), the key blocks (6) and the secondary distribution information file (7) are combined to generate and store or transmit two or more packages (8). When the electronic information is used, the primary distribution information file (4) is restored on the basis of the secondary distribution file (7) to restore the electronic information file (1) on the basis of the primary distribution information file (4).

[続葉有]

WO 02/27501 A1

(57) 要約:

電子情報ファイル１を複数の情報エレメント２に分割し順序を変えて組み合わせることにより２個以上の情報ブロック３を生成し情報エレメント２の分割再配置方法に関する情報を保持する一次分配情報ファイル４を生成し、一次分配情報ファイル４を電子情報ファイル１と同様にキーフラグメント５に分割し再配置してキーブロック６を作成し、一次分配情報ファイル４の分割再配置方法に関する情報を保持する二次分配情報ファイル７を生成し、情報ブロック３とキーブロック６と二次分配情報ファイル７を組み合わせて２個以上のパッケージ８を生成して格納もしくは伝送し、電子情報を使用するときに二次分配情報ファイル７に基づいて一次分配情報ファイル４を復元し、一次分配情報ファイル４に基づいて電子情報ファイル１を復元する。

明細書

電子情報の編成復元方法

技術分野

この発明は、電子情報の保管あるいは通信における電子情報の安全確保方法に関する。

背景技術

多数のコンピュータが通信網に接続されてシステムを形成するようになって、各コンピュータが通信路を介して不特定多数の人と連結されうるようになってきた。このため、ハードディスク装置などコンピュータの外部記憶装置に格納した電子情報も通信路を介して権利のない他人にアクセスされて盗用や改竄をされる心配がある。

また、電子メール、クレジットカード番号、パスワードその他の個人情報交換、ゲームプログラムやビジネスプログラムなどのアプリケーションプログラムの配布、データベースから抽出編集されたデータの配布など、電子情報を通信路を用いて伝送することが多くなってきた。このような電子情報交換に外部に解放された通信環境を使用する場合には、傍受あるいは窃盗行為などにより受信者でない他人が通信中の電子情報を入手して利用する可能性がある。特に有料で情報を配布する場合やプライバシーに係わる情報を伝送する場合には、通信中の電子情報を容易に盗用されないようにする必要がある。

通信中や保管中の電子情報を入手しても無関係の他人が利用できなければよいため、暗号化により電子情報の秘密性を確保する方法が行われている。このような目的に開発された暗号化技術は、対称鍵を用いた暗号方式、非対称鍵を用いた暗号方式、それぞれ多様に存在する。

しかし、これら暗号化技術を用いても、保管されている電子情報や伝送されている電子情報に全ての情報が含まれている限り、暗号の解読など何らかの手段で復号方法を入手した者があれば、容易に復元して有用な情報を入手することができる。また、情報の改竄や偽造も可能で、取り出したり受け取った電子情報が真

正な情報を維持しているか否かを常に心配しなければならない。特に本人認証データや高度な個人情報あるいは企業情報など、高い秘匿性が要求される電子情報を保管したり伝送する場合に、従来方法では不安がある。

そこで、本願発明の発明者は既にＰＣＴ／ＪＰ９９／０１３５０によって、電子情報ファイルを多数の情報エレメントに分割し、順序を変えて組み合わせることにより数個の情報ブロックを生成して個別に送信もしくは外部記憶装置に格納する方法を開示している。情報ブロックを生成する際、各々の情報エレメントの大きさや情報エレメントを組み合わせた順序に関する情報を保持する分割抽出データを作成し、情報ブロックおよび分割抽出データを個別に送信もしくは外部記憶装置に保存する。電子情報ファイルを復元する際は、分割抽出データに基づいて情報ブロック内の情報エレメントを切り出し、正しい順序に並べ直して結合する。

この方法によれば、個々の情報ブロックが持つ情報は電子情報全体の一部でしかなく、また分割された断片の集合でしかないため、もし情報ブロックが窃取されてもその情報価値は減殺されている。

しかし、情報ブロックとともに分割抽出データを窃取され、情報ブロック内の情報エレメントを正しく並べ直すことができた場合は、少なくとも情報の一部を傍受者に正しく知られてしまう可能性がある。

また、分割抽出データには各々の情報エレメントの元の電子情報ファイル内での位置が記述してある。したがって、分割抽出データと情報ブロックが窃取された場合、傍受者に窃取した情報ブロック内の情報エレメントが元の電子情報ファイルのどの位置に当たるのかを正確に知られ得るので、有用な情報断片を入手されたり、傍受者に元の電子情報の全容を推定する手がかりを与えることがある。

発明の開示

本発明の電子情報の編成復元方法は、電子情報ファイルを複数の情報エレメントに分割し、分割された情報エレメントから任意の情報エレメントを選択し、順序を変えて組み合わせることにより２個以上の情報ブロックを生成する。この情報ブロックは、全ての情報ブロックを統合すると全ての情報エレメントが含まれ

るようにする。また、情報エレメントへの分割方法と情報ブロックの形成方法を記録した一次分配情報ファイルを生成する。さらに、一次分配情報ファイルを同様に複数のキーフラグメントに分割し、再配分してキーブロックを生成し、キーフラグメントへの分割方法とキーブロックの形成方法を記録した二次分配情報ファイルを生成する。

情報ブロックに適宜キーブロックおよび二次分配情報ファイルを添付して２個以上のパッケージとし、個別に受信者に送信もしくは外部記憶装置に保存する。なお、パッケージを作成する際、全てのパッケージを統合すると全ての情報ブロックとキーブロックが含まれるようにする。また、二次分配情報ファイルは容易に復元できる方式で分割し、一部もしくは全部のパッケージに梱入するようにしてもよい。

電子情報を利用する際は、パッケージから二次分配情報ファイルを切り出し、二次分配情報ファイルに基づいてパッケージに含まれているキーブロックをキーフラグメントに再分割し、正しい順序に並べ直して結合することで一次分配情報ファイルを復元する。さらに、一次分配情報ファイルに基づいて同様にパッケージ内の情報ブロックから情報エレメントを再分割し結合して電子情報ファイルを復元する。

本発明の電子情報の編成復元方法によれば、もしパッケージのいくつかと二次分配情報ファイルを窃取されても、すべてのパッケージが窃取されない限り一次分配情報ファイルを復元されることがないため、情報ブロックから情報エレメントを切り出し、情報を正しく復元されることはない。また、窃取者は一次分配情報ファイルを復元しない限り窃取した情報が電子情報全体のどの位置に相当するかを知ることができないため、窃取したパッケージから情報の一部を復元したり、電子情報の全容を推定することができない。

したがって、一次分配情報ファイルを分割したため、もしパッケージのいくつかが窃取されても情報の復元もしくは推定が非常に困難であり、情報を盗用される可能性が著しく低いので、本発明の電子情報の編成復元方法を用いれば確実に情報の安全を確保することができる。

なお、二次分配情報ファイルを窃取されても一次分配情報ファイルを復元しな

い限り情報ブロックを正しく復元することができないため、二次分配情報ファイルの管理に厳重に注意する必要はなく、二次分配情報ファイルを分割したり暗号を施す等の処理をしなくても特段の問題は生じない。

本発明の電子情報の編成復元方法をアプリケーションプログラムやデータベースのオンライン販売に用いれば、正当な購買者以外の者が通信中の電子情報を窃取してもデータを復元することができないので、プログラムを実行することができず、また有用な情報を取得することができない。したがって通信中の電子情報を窃取する動機がないため、販売者の利益が窃取により損なわれることがない。

また、本人認証データを送付するために適用すれば、もし電子情報を摂取されてもデータの一部をも復元されることがないため、特に安全性の高い情報交換ができる。

図面の簡単な説明

第１図は本発明の電子情報の編成復元方法のうち送信側での手順を説明するブロック図である。第２図は本発明の電子情報の安全確認方法のうち送信側での手順を示すフローダイヤグラムである。第３図は本発明の電子情報の編成復元方法のうち受信側での手順を説明するブロック図である。第４図は本発明の電子情報の安全確認方法のうち受信側での手順を示すフローダイヤグラムである。

発明を実施するための最良の形態

本発明の電子情報の編成復元方法は、電子情報の保管あるいは通信において電子情報の安全を確実に確保する方法である。本発明の方法により、保管中や通信途中で電子情報を窃取する者があっても窃取によって入手できる情報の復元や推定を困難にして情報の有する価値を小さくし窃盗の被害を防ぐ。

以下、図面を参照して本発明の詳細を説明する。

第１図は本発明の電子情報の編成復元方法における電子情報編成方法を説明するブロック図である。また、第２図は本発明の電子情報編成手順を示すフローダイヤグラムである。説明の便宜のため、電子情報ファイルを６個の情報エレメントに分割し２個の情報ブロックに分けた場合を例示している。

本発明の電子情報の編成方法では、対象とする電子情報ファイル１を取り込み（ｓ１）、適当な数の情報エレメント２に分割する（ｓ２）。ここでは、簡単のため、６個の情報エレメントＡ，Ｂ，Ｃ，Ｄ，Ｅ，Ｆに分割している。情報エレメント２は情報として意味がある位置で区切る必要はなく、盗用された時の危険を小さくするためには、電子情報ファイル１を単に物理的に分割したものである方が好ましい。

分割した情報エレメントＡ，Ｂ，Ｃ，Ｄ，Ｅ，Ｆの配列順を変更し適当にグループ化して適当数の、ここでは２個の情報ブロック３を形成する（ｓ３）。

図示した例では、第１の情報ブロック３に情報エレメントＡ，Ｄ，Ｅを配分し、第２の情報ブロック３に情報エレメントＢ，Ｃ，Ｆを配分した。情報ブロック３内の情報エレメントの個数も配列順も任意に選択することができる。

情報ブロック３を形成すると同時に、各々の情報エレメント２の長さ情報や情報ブロック３への組み込み順序等を記録した一次分配情報ファイル４を作成する（ｓ４）。

一次分配情報ファイル４を電子情報ファイル１と同様の操作でキーフラグメント５に分割し（ｓ５）、キーブロック６に配分する（ｓ６）。ここでは、ａ～ｄの４個のキーフラグメントに分割し、ｃ・ａ、ｂ・ｄの２個のキーブロックに配分しているが、キーフラグメントの分割数やキーブロックへの配分順序も任意に選択できる。なお、情報ブロック３と同じ数のキーブロックを形成すると便利である。

さらに、キーフラグメント５の長さ情報やキーブロック６への組み込み順序等を記録した二次分配情報ファイル７を作成する（ｓ７）。なお、二次分配情報ファイル７は図中では記号ｋを付した。

生成した情報ブロック３とキーブロック６と二次分配情報ファイル７とを任意に組み合わせて２個以上のパッケージ８を作成し（ｓ８）、個別に受信者に送信もしくは外部記憶装置に保存する（ｓ９）。安全性のためには、各々のパッケージを別の通信路を用いて送信することや、他の記憶装置に保存することが好ましい。

たとえば、パッケージ８の１つは情報エレメントＣ、Ａ、Ｅ、キーフラグメン

トｂ、ｄおよび二次分配情報ファイルｋを保持し、もうひとつのパッケージ８は情報エレメントＢ、Ｆ、Ｄ、キーフラグメントｃ、ａおよび二次分配情報ファイルｋを保持している。また、それぞれのパッケージ８は含まれる情報の構造を明らかにするヘッダーｈを付帯している。

このような構成を有するパッケージ８では、例えば第２のパッケージの場合、各々の情報エレメントＢ、Ｆ、Ｄが保持している情報は元の電子情報ファイル１のごく一部であるうえ、二次分配情報ファイルｋからキーフラグメントｃ、ａを用いて一次分配情報ファイル４の一部を復元しても、情報ブロック３内での情報エレメントＢ、Ｆ、Ｄの区切りの位置、情報エレメントＢ、Ｆ、Ｄそれぞれの間の関係、個々の情報エレメントが電子情報ファイル１中のどの位置に当たる情報を保持しているか等を伺い知ることはできない。

このように元の電子情報ばかりでなく電子情報の分配情報をさらに分割抽出することにより、元の電子情報の復元を殆ど不可能にしたため１つのパッケージ８から得られる情報は著しく小さくなる。

一般に、情報の窃取の機会が多いのは送信もしくは保存中であるが、本発明の電子情報の編成方法では電子情報をパッケージ８の状態にして送信もしくは保存するため、他人に窃取されたとしても情報の価値が著しく減殺されており、情報を窃取する動機が弱く盗用の危険が小さい。

第３図は本発明における電子情報の復元方法を説明するブロック図である。また、第４図は本発明の電子情報復元の手順を示すフローダイヤグラムである。

電子情報の使用者は、各々のパッケージ８を保管先から取得したり送信者から受信し（ｓ１０）、パッケージ８を全て揃え（ｓ１１）、パッケージ８のヘッダーを参照して先ず二次分配情報ファイル７を切り出す（ｓ１２）。二次分配情報ファイル７にはキーフラグメント５のキーブロック６への組み込み順序や長さ等に関する情報が保存されているため、それに基づいてパッケージ８のキーブロック６部分からキーフラグメント５を切り出し（ｓ１３）、並べ直して一次分配情報ファイル４を復元する（ｓ１４）。

一次分配情報ファイル４には情報エレメント２の情報ブロック３への組み込み順序や情報エレメント２それぞれの長さ等の情報が保存されているため、それに

基づいて情報エレメント２を切り出し（ｓ１５）、並べ直して電子情報ファイル１を復元して元の電子情報を復元する（ｓ１６）。

以上のように、本発明の電子情報の編成復元方法では送信、保存中のパッケージ８を窃取されてもそこから得られる情報が著しく小さいため、安全に情報を通信、保管することができる。

なお、二次分配情報ファイルｋはいずれかのパッケージに含まれていればよいことはいうまでもない。また、二次分配情報ファイルｋをパッケージ８と別途独立に保管あるいは送付するようにしても良い。

本発明の電子情報の編成復元方法では、１個の電子情報ファイル１に対応する情報ブロック３は２個に限らず、３個以上の複数でもよい。同様に、キーブロック６やパッケージ８も２個に限らない。また、全てのパッケージ８に情報ブロック３とキーブロック６の両方を含んでいる必要はない。しかし、安全性の観点から、全てのパッケージ８にキーブロック６を梱入するのが好ましい。さらに、二次分配情報ファイル７を容易に復元できる方式で分割し、複数のパッケージ８に配分して添付してもよい。

また、本発明の電子情報の編成復元方法の手順をコンピューターに実行させるプログラムをコンピューターで読み取り可能な記憶媒体に記録して使用しもしくは配布してもよい。

産業上の利用可能性

以上詳細に説明した通り、本発明の電子情報の編成復元方法は、電子情報ファイルを情報エレメントに分割し再配置して情報ブロックに分納し、その分割再配置方法に関する情報を保持する一次分配情報ファイルを生成し、一次分配情報ファイルをキーフラグメントに分割してキーブロックに分納し、一次分配情報ファイルの分割再配置方法に関する情報を保持する二次分配情報ファイルを作成し、情報ブロック、キーブロック、二次分配情報ファイルを適宜同梱して２個以上のパッケージを生成し、通信路に置いたり記憶装置に納めるので、外部の者が通信途中や格納中の情報ブロックを窃取しても、小さな情報エレメントがバラバラに収納されていて電子情報の内容を判読することができず、秘密の漏洩を防ぐこと

ができる。

請求の範囲

1．電子情報ファイルを複数の情報エレメントに分割し、分割された該情報エレメントを選択し順序を変えて組み合わせることにより全ての情報ブロックを統合すると全ての情報エレメントが含まれるような２個以上の情報ブロックを生成し、また前記情報エレメントへの分割方法と情報ブロックの形成情報を記録した一次分配情報ファイルを生成し、該一次分配情報ファイルを複数のキーフラグメントに分割し、分割された該キーフラグメントを選択し順序を変えて組み合わせることにより全てのキーブロックを統合するとすべてのキーフラグメントが含まれるような２個以上のキーブロックを生成し、前記キーフラグメントとキーブロックの形成情報を記録した二次分配情報ファイルを生成し、前記情報ブロックとキーブロック、もしくは前記情報ブロックとキーブロックと二次分配情報ファイルを同梱して複数のパッケージを作り、該パッケージを個別に格納もしくは伝送することを特徴とする電子情報の編成方法。

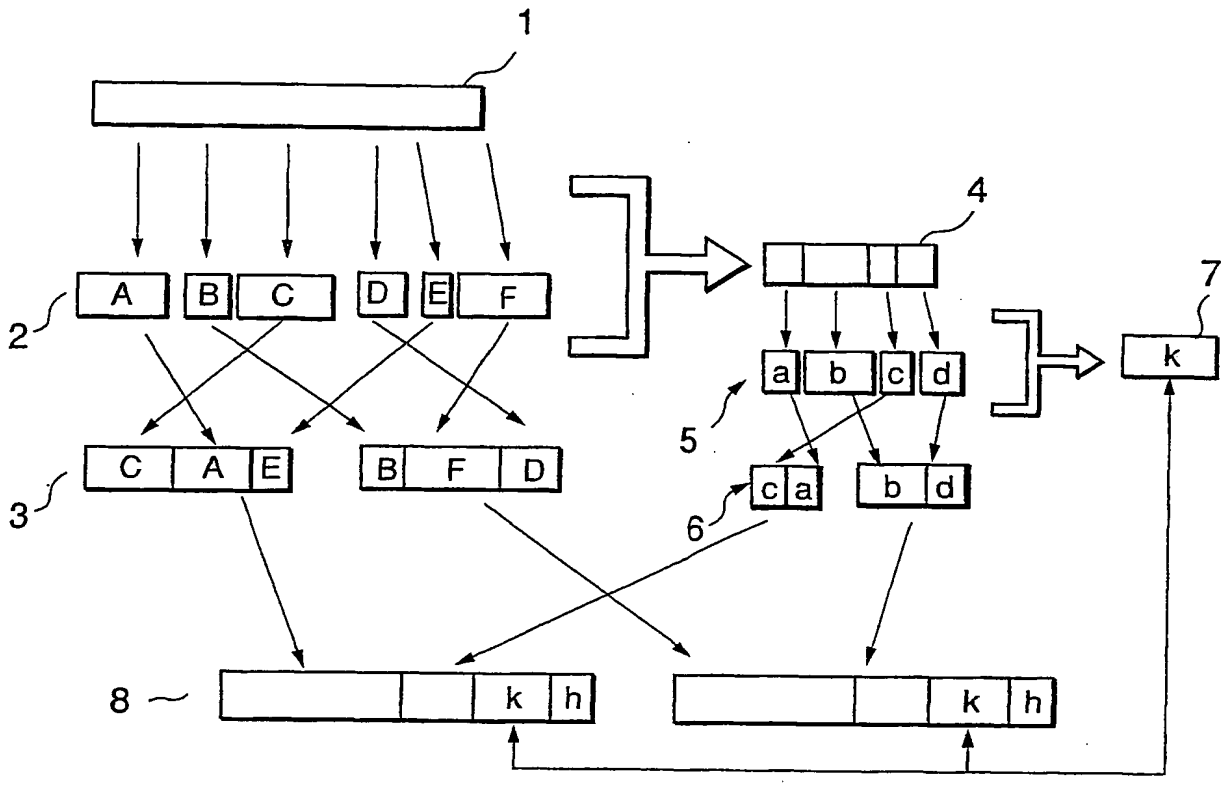
2．請求の範囲第１項に記載の電子情報の編成方法により編成されたパッケージをすべて受信もしくは読み出して集合し、該パッケージから二次分配情報ファイルを切り出し、該二次分配情報ファイルに基づいてキーブロックに含まれるキーフラグメントを再分割し正しい順序に並べ直して統合し一次分配情報ファイルを復元するとともに、該一次分配情報ファイルに基づき情報ブロックに含まれる情報エレメントを再分割し正しい順序に並べ直して統合し電子情報ファイルを復元することを特徴とする電子情報の復元方法。

3．電子情報ファイルを複数の情報エレメントに分割させる手順と、分割された該情報エレメントを選択し順序を変えて組み合わせることにより全ての情報ブロックを統合すると全ての情報エレメントが含まれるような２個以上の情報ブロックを生成させる手順と、前記情報エレメントと情報ブロックの形成情報を記録した一次分配情報ファイルを生成させる手順と、該一次分配情報ファイルを複数のキーフラグメントに分割し分割された該キーフラグメントを選択し順序を変えて組み合わせることにより全てのキーブロックを統合するとすべてのキーフラグメントが含まれるような２個以上のキーブロックを生成させる手順と、前記キーフラグメントとキーブロックの形成情報を記録した二次分配情報ファイルを生成さ

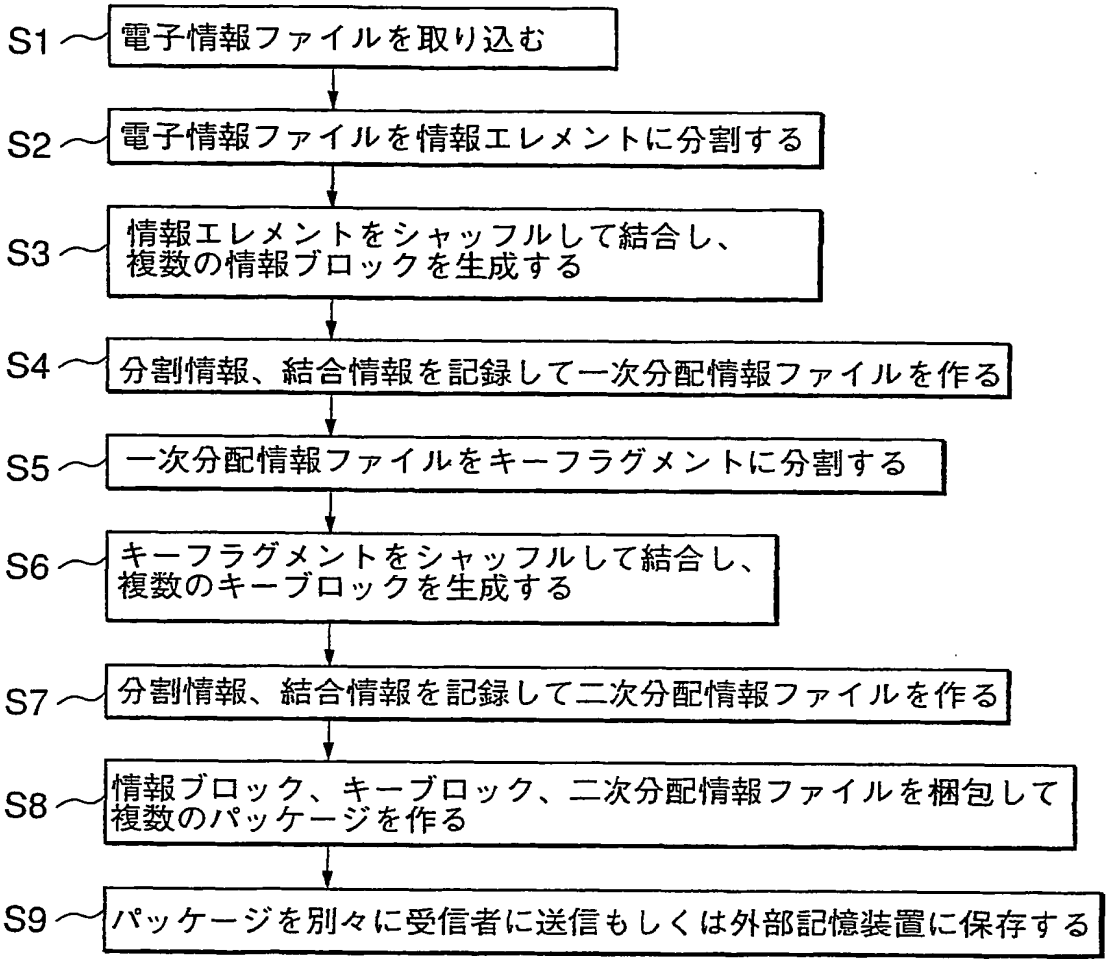
せる手順と、前記情報ブロックとキーブロック、もしくは前記情報ブロックとキーブロックと二次分配情報ファイルを同梱して複数のパッケージを作らせる手順と、該パッケージを個別に格納もしくは伝送させる手順とをコンピューターに実行させるプログラムを記録したコンピューター読み取り可能な記録媒体。

4．請求の範囲第3項に記載のプログラムに基づいて編成されたパッケージをすべて受信もしくは読み出して集合させる手順と、該パッケージから二次分配情報ファイルを切り出させる手順と、該二次分配情報ファイルに基づいてキーブロックに含まれるキーフラグメントを再分割し正しい順序に並べ直して統合し一次分配情報ファイルを復元させる手順と、該一次分配情報ファイルに基づき情報ブロックに含まれる情報エレメントを再分割し正しい順序に並べ直して統合し電子情報ファイルを復元させる手順とをコンピューターに実行させるプログラムを記録したコンピューター読み取り可能な記録媒体。

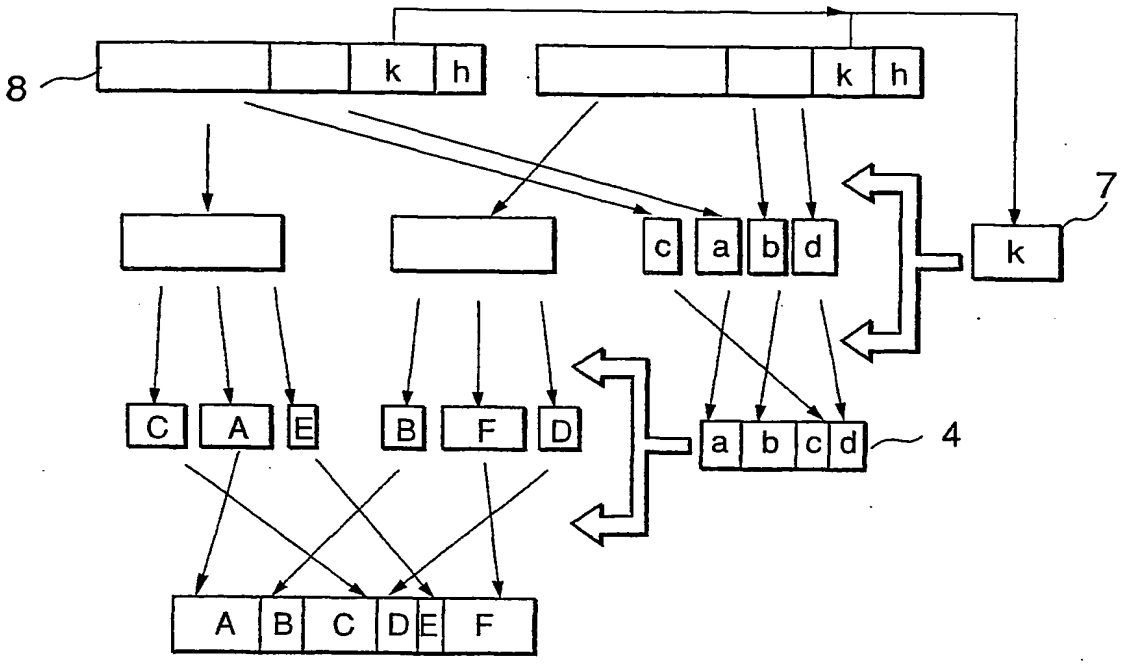
第 1 図



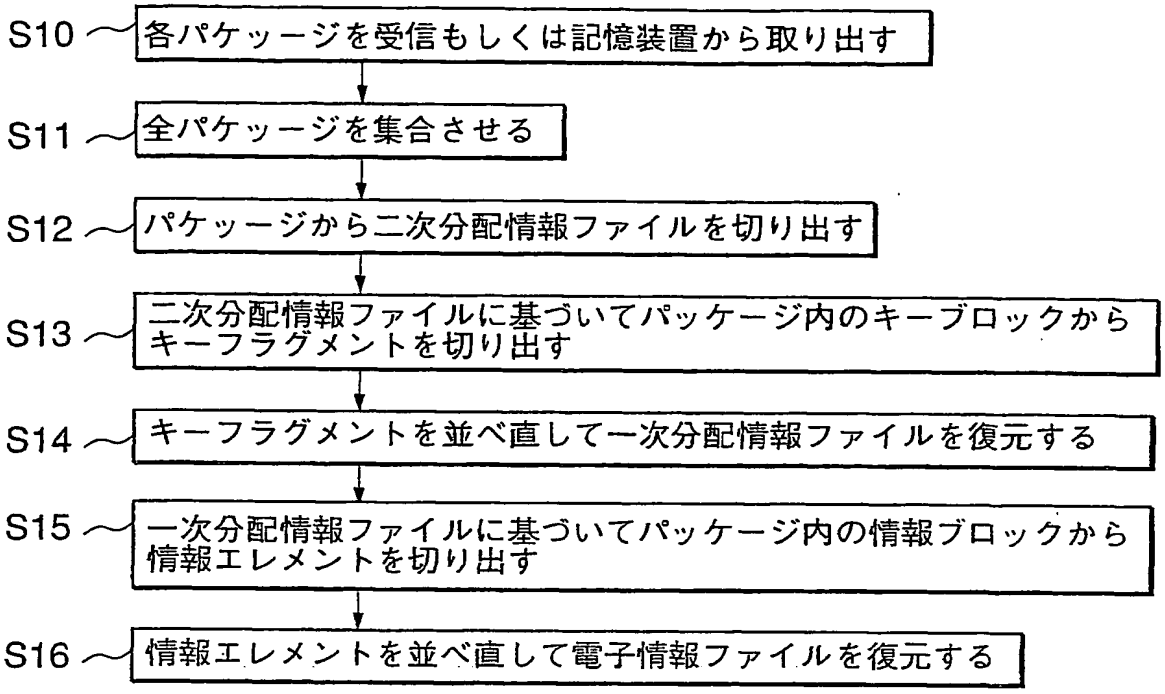
第 2 図


S1
電子情報ファイルを取り込む
S2
電子情報ファイルを情報エレメントに分割する
S3
情報エレメントをシャッフルして結合し、
複数の情報ブロックを生成する
S4
分割情報、結合情報を記録して一次分配情報ファイルを作る
S5
一次分配情報ファイルをキーフラグメントに分割する
S6
キーフラグメントをシャッフルして結合し、
複数のキーブロックを生成する
S7
分割情報、結合情報を記録して二次分配情報ファイルを作る
S8
情報ブロック、キーブロック、二次分配情報ファイルを梱包して
複数のパッケージを作る
S9
パッケージを別々に受信者に送信もしくは外部記憶装置に保存する

第 3 図



第 4 図


S10
各パケッージを受信もしくは記憶装置から取り出す
S11
全パケッージを集合させる
S12
パケッージから二次分配情報ファイルを切り出す
S13
二次分配情報ファイルに基づいてパッケージ内のキーブロックから
キーフラグメントを切り出す
S14
キーフラグメントを並べ直して一次分配情報ファイルを復元する
S15
一次分配情報ファイルに基づいてパッケージ内の情報ブロックから
情報エレメントを切り出す
S16
情報エレメントを並べ直して電子情報ファイルを復元する